We claim:

1. A secure key replacement protocol (SKRP), comprising:

receiving a rekey request, wherein the rekey request identifies a private key for replacement, the rekey request, comprising:

a SKRP key, and

a challenge;

authenticating the rekey request;

replacing the identified private key with the SKRP key;

signing the challenge with the SKRP key; and

returning the signed challenge.

2. The secure key replacement protocol of claim 1, wherein the rekey request is received at a removable device.

3. The secure key replacement protocol of claim 2, wherein the removable device comprises one of a magnetic card, a smart card, and a token.

4. The secure key replacement protocol of claim 2, wherein the removable device is coupled to a user's computer.

5. The secure key replacement protocol of claim 1, wherein the rekey request is received at a user's computer.

6. The secure key replacement protocol of claim 1, further comprising deleting the SKRP key.

7. The secure key replacement protocol of claim 1, further comprising preventing a replay attack.

8. The secure key replacement protocol of claim 7, wherein preventing a replay attack, comprises:

determining a time stamp on the rekey request;

comparing the time stamp to a current time; and

rejecting the rekey request when the time stamp differs from the current time by a specified limit.

9. The secure key replacement protocol of claim 8, wherein the specified limit is 24 hours.

10. The secure key replacement protocol of claim 7, wherein preventing a replay attack, comprises:

reading a key identifier of the private key;

comparing the read key identifier to key identifiers of previously deleted private keys; and

rejecting the key request if the read key identifier matches any of the key identifiers of previously deleted keys.

11. The secure key replacement protocol of claim 1, wherein receiving the rekey request comprises receiving the key request from a certificate authority, and wherein returning the signed challenge comprises returning the signed challenge to the certificate authority.

12. The secure key replacement protocol of claim 11, wherein the certificate authority is located at an Internet web site.

13. The secure key replacement protocol of claim 1, wherein authenticating the key request comprises checking a digital signature of the key request.

14. The secure key replacement protocol of claim 1, wherein the private key allows access to one or more documents.

15. The secure key replacement protocol of claim 1, wherein the private key allows execution of transactions comprising one of on-line banking, on-line purchasing, and viewing web site content.

16. A method for secure replacement of private keys, comprising:

sending a rekey request to a user terminal, the rekey request comprising:

identifiers of one or more private keys to be replaced,

secure key replacement protocol (SKRP) keys to replace the private keys, and

a challenge to be signed at the user terminal; and

receiving the signed challenge.

17. The method of claim 16, wherein the rekey request further comprises a time stamp, wherein the time stamp is compared to a current time at the user terminal.

18. The method of claim 16, wherein sending the rekey request comprises sending the rekey request from an Internet web site.

19. The method of claim 16, wherein the user terminal is a node on a computer network, and wherein sending the rekey request comprises sending the rekey request from another node on the computer network.

20. The method of claim 16, wherein the private keys are stored on a removable device, the removable device adapted for insertion into the user terminal, further comprising receiving an indication from the user terminal when the removable device is inserted into the user terminal.

21. An apparatus that provides secure key replacement (SKR), comprising:

a receiving module that receives and processes a SKR request, the SKR request comprising:

an identity of a private key to be replaced,

a SKR key to replace the private key, and

a challenge that, when signed, indicates the private key is replaced with the SKR key;

an authentication module that checks authenticity of the SKR request;

a rekey module that replaces the private key with the SKR key and signs the challenge; and

a return module that returns the signed challenge.

22. The apparatus of claim 21, further comprising prevention means to prevent a replay attack.

23. The apparatus of claim 22, wherein the SKR request further comprises a time stamp indicative of a time of issuance of the SKR request, and wherein the prevention means, comprises:

a program, operable to read the time stamp on the SKR request and to compare the time stamp to a current time.

24. The apparatus of claim 22, wherein the prevention means comprises:

a memory that stores identities of previously deleted private keys; and

a program that compares the identity of the private key to be replaces with the identities of the previously deleted private keys.

25. The apparatus of claim 21, wherein the receiving module, the authentication module, the rekey module and the return module are implemented on a removable device capable of insertion into a user terminal.

26. The apparatus of claim 25, wherein the removable device is one of a magnetic card, a smart card, and a token.

27. The apparatus of claim 25, wherein the user terminal is a computer operating in a communications network, and wherein the SKR request is provided by a certificate authority coupled to the communications network.